Claims

We claim:

1. A method for securing a file, the method comprising:

launching an application when a request to access the file is received;

determining, in an operating system supporting the application, whether the file being accessed is secured;

when the file is determined to be secured,

activating a cipher module and loading the file through the cipher module into the application;

when the file is determined to be non-secured,

loading the file into the application without activating the cipher module.

2. The method of Claim 1, wherein the cipher module, once activated, operates within the operating system.

3. The method of Claim 1, wherein the cipher module, once activated, operates transparently to a user requesting an access to the file.

4. The method of Claim 1, wherein the secured file includes a header and an encrypted portion, the header including or pointing to security information including a file key that, once obtained, can be used to decrypt the encrypted portion.

5. The method of Claim 4, wherein the determining of whether the file being accessed is secured comprises determining if the file being accessed includes the header.

6. The method of Claim 4, wherein the header further includes a flag indicating that the file being accessed is secured, and wherein the determining of whether the file being accessed is secured comprises determining if the file has the flag.

7. The method of Claim 4, wherein the loading of the file through the cipher module into the application comprises:

    retrieving the file key;

    decrypting the encrypted portion with the file key in the cipher module; and

    sending the file in clear mode to the application.

8. The method of Claim 7, wherein the security information including the file key is encrypted with a user key; and wherein the retrieving of the file key comprises:

    obtaining a user key associated with a user requesting an access to the file; and

    decrypting the encrypted security information with the user key to retrieve the file key.

9. The method of Claim 8, wherein the security information further includes access rules controlling how and who the secured file can be accessed.

10. The method of Claim 9, wherein the loading of the file through the cipher module into the application only happens when access privilege of the user is within permissions granted by the access rules.

11. A method for securing a file, the method comprising:

maintaining a file key in a temporary memory space;

encrypting the file with the file key in a cipher module to produce an encrypted portion;

preparing security information for the encrypted portion, the security information being encrypted and including the file key and access rules to control access to the encrypted portion; and

attaching the encrypted security information to the encrypted portion.

12. The method of Claim 11 further comprising deleting the file key from the temporary memory space when the attaching of the encrypted security information to the encrypted portion is complete.

13. The method of Claim 11, wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen whenever the file is caused to be stored in a storage space.

14. The method of Claim 11, wherein the encrypting of the file with the file key, the preparing of the security information, and the attaching of the encrypted security information happen upon receiving an instruction from an application or an operating system supporting the application.

15. The method of Claim 14, wherein the application is provided in Microsoft Office and the operating system is Microsoft Windows.

16. The method of Claim 15, wherein the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application.

17. The method of Claim 14, wherein the instruction is generated from an automatic operation of saving the file being opened into the storage space, the automatic operation is either triggered by the application itself or the operating system.

18. The method of Claim 11 further comprising encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group of users.

19. The method of Claim 18 wherein the access rules in the security information comprises user information identifying who can assess the encrypted portion and how the encrypted portion can be accessed.

20. The method for providing access control to a file, the method comprising:

launching an application under an operating system when a request to access the file is received;

forwarding the request to a file system manager in the operating system;

activating a document securing module by the file system manager to determine whether the file being accessed is secured;

activating a cipher module when the file is determined to be secured, and loading the file through the cipher module into the application.

21. The method of Claim 20 further comprising:

retrieving security information from the file when the file is determined to be secured, the security information including a file key and access rules; and

obtaining an access privilege of a user requesting to access the file.

22. The method of Claim 21, wherein the activating of the cipher module proceeds successfully when the access privilege is within permissions granted by the access rules.

23. The method of Claim 22, wherein the activating of the cipher module comprises decrypting an encrypted portion of the secured file with the file key.

24. A software product including computer instructions for securing a file, the instructions, when executed by a processor, cause the processor to perform operations of:

determining, in an operating system, whether the file being accessed is secured when a request to access the file by an application is received;

when the file is determined to be secured,

activating a cipher module that operates in the operating system;

loading the file through the cipher module into the application;

when the file is determined to be non-secured,

loading the file into the application without activating the cipher module.

25. The software product of Claim 24, wherein the secured file includes a header and an encrypted portion, the header including or pointing to security information including a file key that, once obtained, can be used to decrypt the encrypted portion

26. The software product of Claim 24, wherein the determining of whether the file being accessed is secured comprises determining if the file being accessed includes the header.

27. The software product of Claim 26, wherein the loading of the file through the cipher module into the application comprises:

retrieving the file key;

decrypting the encrypted portion with the file key in the cipher module; and

sending the file in clear mode to the application.

28. The software product of Claim 27, wherein the security information including the file key is encrypted with a user key; and wherein the retrieving of the file key comprises:

obtaining a user key associated with a user requesting an access to the file; and

decrypting the encrypted security information with the user key to retrieve the file key.

29. The software product of Claim 28, wherein the security information further includes access rules of how and who the secured file can be accessed.

30. The software product of Claim 29, wherein the loading of the file through the cipher module into the application proceeds only when an access privilege of the user is within permissions granted by the access rules.

31. A software product including computer instructions for securing a file, the instructions, when executed by a processor, cause the processor to perform operations of:

maintaining a file key in a temporary memory space;

encrypting the file with the file key in a cipher module to produce an encrypted file, wherein the file has been opened with an application and the cipher module operates transparently as far as a user executing the application is concerned; and

storing, in a storage space, a secured file including the encrypted file and a header, wherein the header includes or points to security information including the file key.

32. The software product of Claim 31 further comprising deleting the file key from the temporary memory space when the application is caused to close the file.

33. The software product of Claim 32, wherein the encrypting of the file with the file key happens whenever the file is caused to be stored in the storage space.

34. The software product of Claim 32, wherein the encrypting of the file with the file key happens upon receiving an instruction from the application or an operating system supporting the application.

35. The software product Claim 34, wherein the instruction is one of (i) Save, (ii) Close and (iii) Exit, all provided in the application.

36. The software product of Claim 34, wherein the instruction is generated from an automatic operation of saving the file being opened into the storage space, the automatic operation is either triggered by the application itself or the operating system.

37. The software product of Claim 31, wherein the security information further includes access rules of how and who the secured file can be accessed.

38. The software product of Claim 37 further comprising encrypting the security information with a user key associated with a member selected from a group consisting of a user, a device, a software module, and a group.

39. The software product of Claim 18 further comprising attaching the header to the encrypted file, wherein the header includes the security information encrypted in addition to a flag indicating that the file is secured.

40. A computing device for securing a file, the computing device comprising:

an application, when executed, accessing the file that includes security information and an encrypted portion, the security information further including a file key and access rules, and the encrypted portion being an encrypted version of the file;

a cipher module activating upon determining that the file being accessed is secured;

wherein the security information is encrypted and can be decrypted with a user key when authenticated; and

wherein the file key can be retrieved to decrypt the encrypted portion only after the access rules have successfully measured against access privilege of the user.

41. The computing device of Claim 40 further including an operating system supporting operations of the application; and wherein the cipher module is embedded in the operating system.

42. The computing device of Claim 41, wherein the cipher module operates in a path through which the file is caused to pass when accessed by the application.

43. The computing device of Claim 40 further including a memory space and a storage space; and wherein the file key is temporarily kept in the memory space when the file is successfully loaded into the application.

44. The computing device of Claim 43, wherein the file key is deleted from the memory space as soon as the file is wrote back to the storage space.

45. The computing device of Claim 40, wherein the user key becomes authenticated only when the user is authenticated by an authentication process to verify who the user claims to be.

46. The computing device of Claim 40, wherein the computing device is coupled to another computing device over a data network, the user key becomes

authenticated only after the user is successfully logged from the computing device into the another computing device.

47. The computing device of Claim 40, wherein the computing device is provided with means for capturing biometric data of the user, the user key becomes authenticated only after the biometric data is successfully verified to support who the user claims to be.

48. The computing device of Claim 40, wherein the user key becomes authenticated after the computing device receives credential information from the user.

49. The computing device of Claim 48, wherein the credential information includes one of a password entered by the user, biometric information of the user, personalized information about the user.

50. The computing device of Claim 49, wherein the biometric information is captured from a device coupled to the computing device.